Program Cyber Security Plan
Exhibit 5 - Continuous Monitoring Program for National Security Systems

1.0 Purpose

The purpose of this document is to provide the Office of Science (SC) consistent methods to periodically and continuously monitor, test and evaluate the information system security controls for National Security Systems (NSS) to ensure that the controls are effectively implemented. The results of the different methods of monitoring are combined to provide both an SC-wide and a site cyber security posture. Continuous monitoring (i.e., verifying the continued effectiveness of those controls over time), and reporting the security status of the information system to appropriate agency officials, are essential activities within a comprehensive NS information security program as defined by NIST SP 800-37, "*Guide for Security Certification and Accreditation of Federal Information Systems*" and the Office of Science National Security System (NSS) Program Cyber Security Plan (PCSP) Implementation Manual.

2.0 Responsibilities

The roles and responsibilities for implementing this document are described in the Office of Science NSS PCSP and the Office of Science NSS PCSP Implementation Manual.

3.0 Management System Operation

3.1 Overview

The Office of Science implements continuous monitoring activities in accordance with the Federal Information Security Management Act (FISMA) and other Federal requirements to protect its NS information and information systems utilizing the principles and functions of NIST. SC staff (defined but not limited to the aforementioned roles and responsibilities):

1) ensure that continuous monitoring requirements are followed;
2) ensure that continuous monitoring requirements are placed into contracts;
3) provide oversight of SC sites' continuous monitoring of work planning and controls;
4) integrate continuous feedback and improvement mechanisms into their work; and
5) perform the necessary oversight and assessments of both the Federal and contractor cyber security programs.

This MS addresses the requirements for SC personnel in the performance of continuous monitoring functions that are Federal responsibilities. Additionally, it ensures that continuous monitoring requirements and methods of accomplishment are identified, communicated, and implemented by both SC staff and contractors. This includes the oversight, assessment, and evaluation of both Federal staff and contractor performance, and reporting of continuous monitoring performance data to SC and other entities (e.g., U.S. Department of Energy [DOE] and, as appropriate, Federal, state, and local governments). Effective implementation of this MS will ensure the security of information and the information systems for the Office of Science. Continuous monitoring and status reporting is a fair and balanced process leveraging the knowledge of the Science Information Officer in combination with the Integrated Service Centers.

The processes for addressing contractor PCSP performance expectations are outlined in the M&O Contracting Management System Description (MSD).

3.2 Key Functions/Services and Processes

The Office of Science implements continuous monitoring of their NSS cyber security posture through a multi-level approach. This multi-level approach uses periodic site and peer reviews (see Appendix 2), SC-wide and site cyber security metrics, and status reports to monitor performance. At the beginning of each year, the Science Information Officer presents a plan to the Chief Operating Officer (COO) for continuous monitoring of the cyber security posture for National Security systems operated at the Federal sites and laboratories. This plan provides a schedule for site reviews and metrics and status reporting requirements, and is coordinated with the DOE Integrated Service Centers.

3.2.1 Site Review Initiative

The site review process consists of an assessment of the security controls, information, and information system environment at each laboratory or site office. This review is conducted by representatives from SC and other DOE sites, and consists of in-depth interviews with personnel responsible for the security of information and a review of cyber security documentation (see appendix 3) to assure that changes are being properly analyzed, tested and incorporated. Technical controls are also reviewed to assure they are performing as intended and represent the most secure posture suitable for mission requirements. The continuous monitoring of security controls is accomplished in a variety of ways, including independent security reviews, self-assessments, penetration testing, scanning and vulnerability assessment for networked systems, or audits. The site review will verify that configuration management baselines are implemented and current, and that documentation has been updated to reflect any changes.

The Office of Science conducts a site review for each laboratory or site office annually. The Science Information Officer (SIO) will coordinate the site reviews with the Integrated Service Centers and laboratory staff. Exceptions for the annual reviews may be granted to sites undergoing GAO, IG, or OA audits.

3.2.1.1 Configuration Management

Configuration Management (CM) implies administration, technical direction, and surveillance to identify and document functional and physical characteristics of an information system (or devices on a system). Changes to a system (or system devices) must be tracked and documented at a detailed level, and a process for approving changes and verifying compliance with specified requirements implemented. CM ensures the security protection features approved for an information system have been systematically implemented and are maintained. This is accomplished by controlling the implementation or operations of systems and the processes for system maintenance or modification. Under the configuration management task, the following controls are reviewed for the devices that constitute the information system infrastructure:

- Configuration baselines of workstations, servers, and network equipment – assure that the CM baseline is appropriate and maintained;
- Patch management is being implemented consistent with the NSS Cyber Security Program Plan (”Master Plan”); and
- Inventory tracking is being implemented consistent with the NSS Master Plan.

3.2.1.2 Documentation of Information System Changes

Documenting information system changes and assessing the potential impact on the security of the system on an ongoing basis is a requirement to maintain the security accreditation of a system. The objective of the configuration management and control task at the system level is to:

- Document the proposed or actual changes to the information system;
- Determine the impact of proposed or actual changes on the security of the system; and
- Document major applications or general support systems added to the infrastructure.

SC requires that any relevant information about a proposed or actual change to the hardware, firmware, or software (such as version or release numbers, descriptions of new or modified features or capabilities, and security implementation guidance) is recorded. It also requires a record of any changes to the information system environment, such as modifications to the facility. The information system owner and Information System Security Officer (ISSO) should use this information to assess the potential security impact of the proposed or actual changes to the information system. Significant changes to the information system should not be undertaken prior to assessing the security impact of such changes and receiving DAA approval to implement the change.

3.2.2 Metrics

3.2.2.1 Metrics Collection

The Office of Science has developed SC-wide metrics to provide a global view of the cyber security posture of National Security activities at Federal sites and the laboratories.

SC-wide metrics are gathered annually. Site metrics illustrating the cyber security posture of a specific site are gathered on a quarterly basis. Both sets of initial metrics are shown in Section 5.0 of this document. They may be adjusted to address new issues or changes in policy as they arise.

The Science Information Officer or designee coordinates with the Integrated Service Centers to determine how metrics are gathered, analyzed, and presented to management. Efforts are made to gather information from existing sources and pre-populate the metrics, where applicable, before transmitting them to the Federal sites and laboratories.

3.2.2.2 Site Metrics

The objective of site metrics is to select an appropriate set of security controls that reflect the security posture of the information systems within a laboratory, site office or HQ. The continuous monitoring of security controls helps to identify potential security-related problems in the information system that are not identified during the site review process conducted as part of the configuration management and control process.

These metrics assure that the laboratories, site offices, Integrated Service Centers, and SC Headquarters regularly review/analyze audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, report findings to the appropriate officials, and take necessary corrective actions.

The criteria established by SC reflect the organization’s priorities and the importance of the information system to the Department. The security controls being monitored are periodically reviewed to ensure that a representative sample of controls which best reflects the security posture of facilities is included in the ongoing security assessments.

3.2.3 Monthly Status Reporting and Documentation Update

Status reporting and documentation are key elements within a robust cyber security program, and provide the primary artifacts that the controls in place work. SC is committed to ensure that configuration standards are maintained and documented. Policies and procedures used to inform personnel on the proper use of National Security information and information systems should be readily available for reference.

Monthly cyber security status reports will be delivered to the Laboratory Director who will transmit the reports to the Site Office Manager, DAA, the Manager of the Integrated Service Center (which has cognizance over that specific site or laboratory), and the Science Information Officer. The Science Information Officer will develop a consolidated status for the COO.

The objectives of the status reporting task are to:

- ensure that the CSPP is updated to reflect proposed or actual changes to the information system.
- ensure that the Plan of Action and Milestones is updated to reflect the activities carried out during the continuous monitoring phase.
- report the security status of the information system and changes to the risks to the DAA and Site/Laboratory Management.
- ensure that cyber security is responsive to evolving threats and vulnerabilities.
- highlight any cyber security incidents, issues identified during audits, inspections, or self assessments, and disseminate the approach to their remediation throughout SC.

4.0 Requirements

The following table summarizes high-level requirements relevant to this management system.

Document Number	Title
P.L. 103-356	Government Management Reform Act of 1994, (October 13, 1994)
P.L. 104-208	Title VIII, Federal Financial Management Improvement Act of 1996 (FFMIA), (October 1, 1996).
P.L. 104-231	Electronic Freedom of Information Act (e-FOIA), (October 2, 1996)
P.L. 107-347	Title III, Federal Information Security Management Act of 2002 (FISMA), (December 17, 2002).
P.L. 93-579	Privacy Act of 1974, as amended [Title 5 United States Code (U.S.C.) Section 552a], (December 31, 1974).
P.L. 96-349	Trade Secrets Act - (18 U.S.C., section 1905), (January 22, 2002).
P.L. 97-255	Federal Managers' Financial Integrity Act of 1982 (FMFIA), (September, 8, 1982)
P.L. 99-474	Computer Fraud and Abuse Act (18 U.S.C. section 1030), (October 16, 1986)
P.L. 99-508	Electronic Communications Privacy Act of 1986, (October 21, 1986)
P.L. 100-235	Computer Security Act of 1987, (January 8, 1988)
P.L. 104-106	Division E, Clinger-Cohen Act (Information Technology Management Reform Act of 1996), (February 10, 1996)

OMB Circular A-123	Management Accountability and Control, (August 4, 1986) (revised Dec 21, 2004)
OMB Circular A-130 Appendix III	Security of Federal Automated Information Resources, (November 2003)
OMB Memorandum M-96-20	Implementation of the Information Technology Management Reform Act of 1996, (April 4, 1996)
OMB Memorandum M-97-02	Funding Information Systems Investments, (October 25, 1996)
OMB Memorandum M-99-20	Security of Federal Automated Information Resources, (June 2 3, 1999)
OMB Memorandum M-00-07	Incorporating and Funding Security in Information Systems Investments, (February 28, 2000)
OMB Memorandum M-00-10	OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act, (April 25, 2000)
OMB Memorandum M-00-015	OMB Guidance on Implementing the Electronic Signatures in Global and National Commerce Act, (September 25, 2000)
OMB Memorandum M-01-08	Guidance on Implementing the Government Information Security Reform Act, (January 16, 2001)
OMB Memorandum M-01-26	Component-Level Audits, (July 10, 2001)
OMB Memorandum M-04-25	FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, (July 17, 2006)
OMB Memorandum M-05-02	Financial Management Systems, (December 1, 2004)
NIST FIPS 201-1	National Institute of Standards and Technology (NIST) Personal Identity Verification (PIV) of Federal Employees and Contractors, (March 2006)
NIST FIPS 200	Minimum Security Requirements for Federal Information and Information Systems, (March 2006)
NIST FIPS 199	Standards for Security Categorization of Federal Information and Information Systems, (February 2004)
NIST FIPS 142-2	Security Requirements for Cryptographic Modules, (May 2001)

NIST [1]SP 800-92	Guide to Computer Security Log Management, (September 2006)
NIST SP 800-88	Guidelines for Media Sanitization, (September 2006)
NIST SP 800-83	Guide to Malware Incident Prevention and Handling, (November 2005)
NIST SP 800-70	The NIST Security Configuration Checklists Program, (May 2005)
NIST SP 800-65	Integrating Security into the Capital Planning and Investment Control Process, (January 2005)
NIST SP 800-64	Security Considerations in the Information System Development Life Cycle, Revision 1, (June 2004)
NIST SP 800-61	Computer Security Incident Handling Guide, (January 2004)
NIST SP 800-60	Guide for Mapping Types of Information and Information Systems to Security Categories, (June 2004)
NIST SP 800-55	Security Metrics Guide for Information Technology Systems, (July 2003)
NIST SP 800-53A	Guide for Assessing the Security Controls in Federal Information Systems, (April 2006)
NIST SP 800-53 R1	Recommended Security Controls for Federal Information Systems, (December 2006)
NIST SP 800-50	Building an Information Technology Security Awareness and Training Program, (October 2003)
NIST SP 800-47	Security Guide for Interconnecting Information Technology System, (August 2002)
NIST SP 800-37	Guide for the Security Certification and Accreditation of Federal Information Systems, (May 2004)
NIST SP 800-34	Contingency Planning Guide for Information Technology Systems, (June 2002)

[1] Federal Information Processing Standards (FIPS) are developed by NIST in accordance with FISMA. FIPS are approved by the Secretary of Commerce and are compulsory and binding for federal agencies. Since FISMA requires that federal agencies comply with these standards, agencies may not waive their use.

Guidance documents and recommendations are issued in the NIST Special Publication (SP) 800-series. Office of Management and Budget (OMB) policies (including OMB Memorandum M-06-20, FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management) state that for other than national security programs and systems, agencies must follow NIST guidance.

NIST SP 800-30	Risk Management Guide for Information Technology Systems, (July 2002)
NIST SP 800-26, R1	Guide for Information Security Program Assessments and System Reporting Form, (November 2001)
NIST SP 800-18, R1	Guide for Developing Security Plans for Federal Information Systems, (February 2006)
DOE O 142.1	Classified Visits Involving Foreign Nationals, (January 13, 2004)
DOE O 142.3	Unclassified Foreign Visits and Assignments Program, (June 18, 2004)
DOE P 205.1	Departmental Cyber Security Management Policy, (May 8, 2001)
DOE O 205.1A	Department of Energy Cyber Security Management Program, (December 4, 2006)
DOE M 205.1-4	National Security System (NSS) Manual, (March 8, 2007)
DOE 0 221.2	Cooperation with the Office of Inspector General, (March 22, 2001)
DOE P 226.1	Department of Energy Oversight Policy, (June 10, 2005)
DOE O 226.1	Implementation of Department of Energy Oversight Policy, (September 15, 2005)
DOE M 452.4-1A	Protection of Use Control Vulnerabilities and Design, (March 11, 2004)
DOE O 457.1	Nuclear Counterterrorism, (February 7, 2006)
DOE P 470.1	Integrated Safeguards and Security Management (ISSM) Policy, (May 8, 2001)
DOE O 470.2B	Independent Oversight and Performance Assurance Program, (October 31, 2002)
DOE M 470.4-1	Safeguards and Security Program Planning and Management, (August 26, 2005)
DOE M 470.4-2	Physical Protection, (August 26, 2005)
DOE M 470.4-4	Information Security, (August 26, 2005)
DOE M 470.4-5	Personnel Security, (August 26, 2005)
DOE O 471.1	Identification and Protection of Unclassified Controlled Nuclear Information, (June 30, 2000)
DOE O 470.4	Safeguards and Security Program, (August 26, 2005)
DOE O 475.1	Counterintelligence Program, (February 10, 2004)

DOE O 5610.2	Control of Weapon Data, (September 2, 1986)
DoD 5220.22-M	National Industrial Security Program Operating Manual, (February 2006)
E.O. 12958	Classified National Security Information, (April 17, 1995)
E.O. 13011	Federal Information Technology, (July 17, 1996)
HSPD-12	Policy for a Common Identification Standard for Federal Employees and Contractors, (August 27, 2004)

5.0 Subject Areas

5.1 Configuration Management

All device configuration requirements listed in the control sets for the information systems outlined in the SC NSS PCSP Implementation Manual must be **fully met** prior to the system being accredited for operation at SC sites. SC supports using the DISA-approved "gold disk" or other approved configuration management tool for establishing a baseline for configuration settings.

Explanation of Metric: The metric reflects the number of systems that implemented a recognized national standard (gold disk) within their infrastructure. Sites that have implemented a standard configuration on the greatest number of devices possible are considered robust for this metric. Reducing the possibility of users making their own changes is also considered in this metric – sites will be weighed as to whether they have controls which either flag or prevent configuration changes.

What we look at:	*Levels of performance:*
a) evidence of national standard (gold disk)	percentage of devices with a national standard applied (ideal is 100%)
b) number of operating systems used at the site	one, few, many
c) version of operating systems used at the site	number and percentage of devices with an OS currently supported by the vendor
d) restriction of administrative rights	percentage of devices without administration rights (higher is better)

5.2 Metrics for NS Systems at SC Sites

SC- and site-wide metrics for cyber security as a whole are outlined in the SC MSD "*Continuous Monitoring Program for Unclassified Systems*." In addition, all data collection and retention and documentation requirements listed in the control sets for the information systems outlined in the SC NSS PCSP Implementation Manual must be **fully met** prior to the system being accredited for operation at SC sites. Sites are required to maintain metrics documentation for the following. All metrics being reported should be collected as part of the normal "collection cycle" at the facility.

5.2.1 Audit

Explanation of Metric: All access to information should be recorded in log files, and the log files must be reviewed on a periodic basis to assure that the integrity of the access controls is being enforced. Log file review is also a requirement in the event the intrusion detection system identifies malicious or suspicious activities. A robust protection system will be able to identify access to the record level. A robust protection system will have frequent audit reviews.

What we look at:	*Levels of performance:*
a) number of auditable events tracked –per control AU-2	minimum / above minimum
b) frequency of Audit log review	daily, weekly, monthly, longer than monthly
c) number of violations identified	number (smaller is better) these numbers are cumulative annually
D number of violations identified/Number of audit anomalies found (potential security violations	percentage (ideal is zero) these numbers are cumulative annually

5.2.2 Configuration Management

Explanation of Metric: Only system administrators (SA) or ISSO have the authority to change configuration setting on devices (standalone or networked). However there are instances where users may be granted elevated system privileges in order to accomplish the tasks for their job. This metric monitors the changes to the configuration setting of the device to assure that only authorized changes are permitted (see appendix 1 for expected configuration settings). The frequency for which log files will be reviewed for unauthorized changes will be defined in the security plan.

What we look at:	*Levels of performance:*
a) unauthorized changes to the approved baseline	number per system, number per site. (ideal is zero)

5.2.3 Data Protection

Explanation of Metric: This is a companion metric to audit. Not all suspicious activities result in a compromise of information, and not all malicious actions are successful. This metric tracks suspicious and malicious activity relative to the level or access achieved (e.g. none, system level, application level, file level). (Note: the official reporting procedure is defined in cyber security guidance document CS 9 – this metric is only the number reported).

What we look at:	*Levels of performance:*
a) number of malicious actions by incident type	number (ideal is zero) these numbers are cumulative annually
b) number of suspicious activities reported by incident type	number (ideal is zero) these numbers are cumulative annually

5.2.4 Operational Controls

Explanation of Metric: Environments are not static. Devices/workstations are added or decommissioned, new employees are hired who require training, new administrators are hired or promoted and these people need to learn new job functions.

What we look at:	*Levels of performance:*
a) number of systems added, number of systems decommissioned (monthly)	number
b) number of physical access violations	number (ideal is zero) these numbers are cumulative annually
c) number of users with training completed/ number of users	percentage (ideal is 100%)
d) number of SAs with training completed /number of SAs	percentage (ideal is 100%)

5.2.5 Authentication

Explanation of Metric: In a classified environment there should be no “guest access” allowed at any time. This metric monitors if systems are being attacked by insiders that have access to the systems, but no need to know.

What we look at:	*Levels of performance:*
a) number of account lockout by unknown users	number (ideal is zero)

5.2.6 Life Cycle Support (applies only for custom software)

Explanation of Metric: In a classified environment running custom software is it critical that reported software flaws be addressed and corrected, because there is no patching service from the vendor. This metric monitors whether reported flaws are being corrected. In a classified environment all reported flaws need to be resolved and patches implemented.

What we look at:	*Levels of performance:*
a) number of system (software) flaws reported	number (ideal is zero)
b) number of system (software) flaws reported/number of system (software) flaws mitigated	percentage (ideal is 100%). these numbers are cumulative annually.

5.27 Vulnerability Analysis

Explanation of Metric: All sites must identify devices and applications that are not current with updated security patches. Patches that are applied on a timely basis result in the most robust implementation of this control. Standalone systems are NOT vulnerable to network attacks – but may contain viruses that attach themselves to documents that may infect other files on the drive. This metric measures the number of exploits that were successful because of operating systems or applications that were not commensurate with the current patch level within the update cycle for the device as defined in the security plan.

What we look at:	*Levels of performance:*
a) number of successful exploits due to unpatched vulnerabilities outside of the update cycle documented in the risk assessment	number (ideal is zero)
b) number of unpatched vulnerabilities outside of the update cycle	number (ideal is zero)

6.0 References

The following table summarizes high-level references relevant to this management system.

Document Number	Title

P.L. 103-356	Government Management Reform Act of 1994, (October 13, 1994)
P.L. 104-208	Title VIII, Federal Financial Management Improvement Act of 1996 (FFMIA), (October 1, 1996).
P.L. 104-231	Electronic Freedom of Information Act (e-FOIA), (October 2, 1996)
P.L. 107-347	Title III, Federal Information Security Management Act of 2002 (FISMA), (December 17, 2002).
P.L. 93-579	Privacy Act of 1974, as amended [Title 5 United States Code (U.S.C.) Section 552a], (December 31, 1974).
P.L. 96-349	Trade Secrets Act - (18 U.S.C., section 1905), (January 22, 2002).
P.L. 97-255	Federal Managers' Financial Integrity Act of 1982 (FMFIA), (September, 8, 1982)
P.L. 99-474	Computer Fraud and Abuse Act (18 U.S.C. section 1030), (October 16, 1986)
P.L. 99-508	Electronic Communications Privacy Act of 1986, (October 21, 1986)
P.L. 100-235	Computer security Act of 1987, (January 8, 1988)
P.L. 104-106	Division E, Clinger-Cohen Act (Information Technology Management Reform Act of 1996), (February 10, 1996)
OMB Circular A-123	Management Accountability and Control, (August 4, 1986) (revised Dec 21, 2004)
OMB Circular A-130 Appendix III	Security of Federal Automated Information Resources, (November 2003)
OMB Memorandum M-96-20	Implementation of the Information Technology Management Reform Act of 1996, (April 4, 1996)
OMB Memorandum M-97-02	Funding Information Systems Investments, (October 25, 1996)
OMB Memorandum M-99-20	Security of Federal Automated Information Resources, (June 23, 1999)
OMB Memorandum M-00-07	Incorporating and Funding Security in Information Systems Investments, (February 28, 2000)
OMB Memorandum M-00-10	OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act, (April 25, 2000)
OMB Memorandum M-00-015	OMB Guidance on Implementing the Electronic Signatures in Global and National Commerce Act, (September 25, 2000)

OMB Memorandum M-01-08	Guidance on Implementing the Government Information Security Reform Act, (January 16, 2001)
OMB Memorandum M-01-26	Component-Level Audits, (July 10, 2001)
OMB Memorandum M-04-25	FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, (July 17, 2006)
OMB Memorandum M-05-02	Financial Management Systems, (December 1, 2004)
NIST FIPS 201-1	National Institute of Standards and Technology (NIST) Personal Identity Verification (PIV) of Federal Employees and Contractors, (March 2006)
NIST FIPS 200	Minimum Security Requirements for Federal Information and Information Systems, (March 2006)
NIST FIPS 199	Standards for Security Categorization of Federal Information and Information Systems, (February 2004)
NIST FIPS 142-2	Security requirements for Cryptographic Modules, (May 2001)
NIST [2]SP 800-92	Guide to Computer Security Log Management, (September 2006)
NIST SP 800-88	Guidelines for Media Sanitization, (September 2006)
NIST SP 800-83	Guide to Malware Incident Prevention and Handling, (November 2005)
NIST SP 800-70	The NIST Security Configuration Checklists Program, (May 2005)
NIST SP 800-65	Integrating Security into the Capital Planning and Investment Control Process, (January 2005)
NIST SP 800-64	Security Considerations in the Information System Development Life Cycle, Revision 1, (June 2004)
NIST SP 800-61	Computer Security Incident Handling Guide, (January 2004)

[2] Federal Information Processing Standards (FIPS) are developed by NIST in accordance with FISMA. FIPS are approved by the Secretary of Commerce and are compulsory and binding for federal agencies. Since FISMA requires that federal agencies comply with these standards, agencies may not waive their use.

Guidance documents and recommendations are issued in the NIST Special Publication (SP) 800-series. Office of Management and Budget (OMB) policies (including OMB Memorandum M-06-20, FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management) state that for other than national security programs and systems, agencies must follow NIST guidance.

NIST SP 800-60	Guide for Mapping Types of Information and Information Systems to Security Categories, (June 2004)
NIST SP 800-55	Security Metrics Guide for Information Technology Systems, (July 2003)
NIST SP 800-53A	Guide for Assessing the Security Controls in Federal Information Systems, (April 2006)
NIST SP 800-53R1	Recommended Security Controls for Federal Information Systems, (December 2006)
NIST SP 800-50	Building an Information Technology Security Awareness and Training Program, (October 2003)
NIST SP 800-47	Security Guide for Interconnecting Information Technology Systems, (August 2002)
NIST SP 800-37	Guide for the Security Certification and Accreditation of Federal Information Systems, (May 2004)
NIST SP 800-34	Contingency Planning Guide for Information Technology Systems, (June 2002)
NIST SP 800-30	Risk Management Guide for Information Technology Systems, (July 2002)
NIST SP 800-26R1	Guide for Information Security Program Assessments and System Reporting Form, (November 2001)
NIST SP 800-18R1	Guide for Developing Security Plans for Federal Information Systems, (February 2006)
DOE O 142.1	Classified Visits Involving Foreign Nationals,(January 13, 2004)
DOE O 142.3	Unclassified Foreign Visits and Assignments Program, (June 18, 2004)
DOE P 205.1	Departmental Cyber Security Management Policy, (May 8, 2001)
DOE O 205.1A	Department of Energy Cyber Security Management Program, (December 4, 2006)
DOE M 205.1-4	National Security System (NSS) Manual, (March 8, 2007)
DOE 0 221.2	Cooperation with the Office of Inspector General, (March 22, 2001)
DOE P 226.1	Department of Energy Oversight Policy, (June 10, 2005)
DOE O 226.1	Implementation of Department of Energy Oversight Policy, (September 15, 2005)

DOE M 452.4-1A	Protection of Use Control Vulnerabilities and Design, (March 11, 2004)
DOE O 457.1	Nuclear Counterterrorism, (February 7, 2006)
DOE P 470.1	Integrated Safeguards and Security Management (ISSM) Policy, (May 8, 2001)
DOE O 470.2B	Independent Oversight and Performance Assurance Program, (October 31, 2002)
DOE M 470.4-1	Safeguards and Security Program Planning and Management, (August 26, 2005)
DOE M 470.4-2	Physical Protection, (August 26, 2005)
DOE M 470.4-4	Information Security, (August 26, 2005)
DOE M 470.4-5	Personnel Security, (August 26, 2005)
DOE O 471.1	Identification and Protection of Unclassified Controlled Nuclear Information, (June 30, 2000)
DOE O 470.4	Safeguards and Security Program, (August 26, 2005)
DOE O 475.1	Counterintelligence Program, (February 10, 2004)
DOE O 5610.2	Control of Weapon Data (September 2, 1986)
DoD 5220.22-M	National Industrial Security Program Operating Manual (February 2006)
E.O. 12958	Classified National Security Information, (April 17, 1995)
E.O. 13011,	Federal Information Technology, (July 17, 1996)
HSPD-12	Policy for a Common Identification Standard for Federal Employees and Contractors, (August 27, 2004)
CS-01	Management, Operational and Technical Controls Guidance, (July 6, 2006)
CS-02	Certification and Accreditation, (March 24, 2006)
CS-03	Risk Management, (June 30, 2006)
CS-04	Vulnerability Management, (July 31, 2006)
CS-05	Interconnect Agreements, (July 31, 2006)
CS-06	Plans of Actions and Milestones (POA&M), (September 7, 2006)
CS-07	Contingency Planning, (August 26, 2006)
CS-08	Configuration Management, (November 27, 2006)
CS-09	Incident Management, (January 2007)
CS-11	Clearing and Media Sanitization (January 2007)

CS-12	Password Management, (June 30, 2006)
CS-13	Wireless Devices and Information Systems, (June 30, 2006)
CS-14	Portable/Mobile Devices, (January 2007)
CS-15	Personally Owned Devices, (January 2007)
CS-18	Foreign National Access to DOE Information Systems, (January 2007)
CS-20	INFOCON, (December 6, 2006)
CS-23	Peer-To Peer Networking, (December 2006)
CS-24	Remote Access, (January 2007)
CS-37	Security, Testing and Evaluation, (January 2007)
CS-38A	Protection of Sensitive Unclassified Information, including Personally Identifiable Information, (November 2006)

Appendix 1

NSS System Technical Configuration

Standalone		
Control	**Description**	**Action**
AU-2	Start-up and shutdown of the audit function.	Set audit log Success/Failure
	Successful use of the user security attribute administration functions.	Set audit log Success/Failure
	All attempted uses of the user security attribute administration functions.	Set audit log Success/Failure
	Identification of which user security attributes have been modified.	Set audit log Success/Failure
	Successful and unsuccessful logons and logoffs.	Set audit log Success/Failure
	Unsuccessful access to security relevant files including creating, opening, closing, modifying, and deleting those files.	Set audit log Success/Failure
	Changes in user authenticators.	Set audit log Success/Failure
	Blocking or blacklisting user Ids, terminals, or access ports.	Set audit log Success/Failure
	Denial of access for excessive logon attempts.	Set audit log Success/Failure
	System accesses by privileged users.	Set audit log Success/Failure
	Privileged activities at the system console (either physical or logical consoles) and other system- level accesses by privileged users.	Set audit log Success/Failure
	Starting and ending times for each access to the system.	Set audit log Success/Failure
AU-3	The audit record for each event shall contain at least the date and time of the event, type of event, user/role, object acted upon, and the outcome (success or failure) of the event	Verify log

Standalone		
Control	**Description**	**Action**
AU-5	Anti virus software is installed and operational.	Install antivirus software
	Intrusion Detection Software (IDS) is installed and operational for networked systems.	Install IDS
	The IDS will alert security personnel (e.g., system owner, Alternate ISSO, network administrator)] of a potential imminent violation of information system security when system activity is found to match a signature event or event sequence that indicates a potential violation of information system security.	Set alerting on IDS
AU-6	Read access to the audit records shall be prohibited to all users except the ISSO and authorized system administrators.	Remove read access to all except ISSO and SA
AU-7	The stored audit records shall be protected from unauthorized deletion, prevent modification, and ensure that records already written (i.e. to media) will be maintained when the audit storage is exhausted, the system fails, or an attack occurs.	Set permission on audit files to deny deletion
	An alarm (e.g. any clear indication that the pre-defined limit has been exceeded) shall be generated and provided to the ISSO and the authorized system administrator if the audit trail storage exceeds 80% of capacity on networked systems. For standalone systems the user will not be able to process work.	Set audit warning at 80% on networked systems, set to lock when full on standalone
	The information system shall prevent auditable events from being lost (e.g., deleted, overwritten, not recorded), except those taken by the ISSO or authorized system administrator if the audit trail has reached storage capacity.	Set permission on audit files to ISSO or SA only.
	The information system shall cease operations if the audit trail has reached storage capacity. The ISSO is the only person authorized to restart operations once sufficient audit capacity is available.	Set permission on system to only allow ISSO or SA to restart when logs are full
CM-1	Set unique system identifier.	Set unique system identifier as computer name
DP-1	Set permissions on system files and folders.	Limit system file and folder access to ISSO or SA

Standalone		
Control	**Description**	**Action**
DP-2	Set group memberships and privileges.	Set user and group privileges on data files and folders
DP-9	Imported files inherit user and group permissions.	Set permission inheritance (if not automatic)
	Unsupported O/S firewalled if networked.	Segregate legacy systems with a firewall
DP-11	The information system security controls shall ensure that any previous information content of a resource (e.g. cache, RAM, temp file, cookies, deleted page files) is made unavailable upon the allocation of the resource.	Set cache and temp files to clear on logout
DP-12	Upon detection of a data integrity error, the information system security control shall enter a description of the error in the audit log and issue an alarm.	Install integrity check software and set alarm
EN-12	Warning banner installed.	Install DOE warning banner
EN-15/25	Write ability to removable media is controlled.	Limit or disable write to media functions and ports
EN-20	User rights are set to least privilege.	Set user rights to least privilege
EN-21	User/SA/ISSO/DBM roles are separate (not the same person)	Set administrator rights to ensure separation of duties
EN-25	Diskless terminals in open areas do not contain non-volatile memory.	Ensure only clients with volatile memory are installed on unsecured areas
IA-1	The information system security controls shall detect when no more than five (5) consecutive unsuccessful authentication attempts occur related to the last successful session authentication for the indicated user.	Set unsuccessful login attempts to 3
	When the defined number of unsuccessful authentication attempts has been met or surpassed, the information system security controls shall inform the system administrator and disable the user account until it is unlocked by the administrator.	Set lockout for +3 unsuccessful login attempts
IA-6	The information system security controls shall require re-authentication of the user under the conditions of unlocking as a result of locking.	Set control to require authentication upon system unlock

Standalone		
Control	**Description**	**Action**
IA-7	The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	Verify password obfuscation
IA-9	The information system security controls do not allow guest or anonymous users to have access to system resources.	Disable guest and anonymous access
MT-1	The information system security controls limit access and changes to the security functions (configuration setting, audit logs, etc) to authorized systems administrators.	Set permissions on security functions to SA
MT-3	The organization configures the information system to provide only essential capabilities, and specifically prohibits and/or restricts the use of the following functions, ports, protocols, and/or services: [e.g. Peer to Peer, Anonymous FTP].	Disable all unauthorized functions and ports
MT-4	The information system security controls shall permit only authorized SA and ISSOs to modify (delete/clear) the audit logs, or change other authentication data (e.g. passwords).	Set permissions on audit data and remove password change functionality from Power Users
MT-4(1)	The information system security controls shall permit only authorized SA and ISSOs to change the system time.	Set permission on system time to ISSO or SA
MT-5	The information system security controls shall assure only the ISSO and authorized system administrators can revoke security attributes associated with the users within the information system.	Set permission on user attributes to ISSO or SA
	The information system security controls shall enforce the revocation of the attributes in real time (if a standalone system - upon system reboot).	Set system changes to take place immediately.
	Upon revocation of security-relevant authorizations (e.g., disable subject), the system must reassign ownership of objects to approved subjects within the information system.	Set SA permission on all data files and folders
	The information system security controls shall enforce the access rights associated with an object when an access check is made.	Test permissions

Standalone		
Control	**Description**	**Action**
PT-1	The information system controls shall run a suite of self-tests (e.g., hardware page protection, sample communications across a network to ensure receipt, and verifying the behavior of specific control settings by the ISSO or system administrator) during initial start-up, periodically during normal operation, or at the request of the authorized user (e.g., recovery from failed condition/event) to demonstrate the correct operation of the information system security controls.	Set system to self-test on startup
PT-5	The information system security controls shall ensure that the information system security policy enforcement functions (e.g. role based access controls) are invoked and succeed before each function within the information system's control is allowed to proceed.	Set system to deny bypass when security functions fail
PT-6	If third party software is applied as a security control, it is set so that only the administration may change the software setting.	Set permissions on all security relevant software to SA
PT-8	The information system shall fail to a "secure" state.	Set system to fail "closed"
SA-2	The information system security controls prevent further access to the system by initiating a session lock after a maximum of 15 minutes of inactivity. The session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures.	Set screensaver to a maximum of 15 minutes and require password to resume processing
	After the session lock has been activated, the information system automatically terminates a remote session after 15 minutes of inactivity.	Set remote session to lock and require re-authentication after 15 minutes
SA-4	The information system notifies the user, upon successful logon, of the date and time of the last logon.	Set system notification for last logon date and time for current user

Periods Processing		
Control	**Description**	**Action**
IA-3	The information system security controls shall provide a mechanism to verify that secrets meet at least two-factor strong authentication mechanisms prior to granting access to systems and the information and resources managed by that system.	Install and require two factor authentication for all users

Isolated Networks

Control	Description	Action
AU-4	The information system shall have the ability to centralize the analysis of the logs and employ software filters to do the first level sorts/analysis.	Set all systems to send audit logs to central location with filtering/parsing software installed
	The information system shall employ automated mechanisms (e.g. writing to audit log file, issuing alarms to a network console) to alert security personnel of (Excessive login attempts across network; Access to privilege system files, Exceeding data quotas/transfers, Creation of account; Privileged account logged into multiple servers/ devices/applications; Attempts to access unauthorized sites/computers/devices/objects; Unauthorized shutdown/restart of system/device/application; Permission change for user/file/application; Use of privileged commands; and Unauthorized export from system to media).	Set alarm on central system to alert on all listed activities
CS-1	When cryptography is required and used within the information system for other than telecommunications, the information system security controls shall establish and manage cryptographic keys using automated mechanisms.	Install a PKI infrastructure for crypto key management
CS-2	When cryptography is required and used within the information system for other than telecommunications, the information system security controls shall perform [list of cryptographic operations (e.g., password encryption, e-mail encryption, etc.)] in accordance with, AES, Triple-DES, that meet FIPS 140-2.	Set cryptographic keys to an algorithm which meets FIPS 140-2

Isolated Networks		
Control	**Description**	**Action**
DP-3	The information system detects and protects against unauthorized changes to software and information. The organization employs automated tools that provide notification to appropriate individuals upon discovering discrepancies during integrity verification.	Install integrity check software and set notifications
	The organization employs automated tools that provide notification to appropriate individuals upon discovering discrepancies during integrity verification.	Set integrity check software to send notifications when discrepancies are found
EN-8	The organization employs automated tools to support near-real-time analysis of IDS events.	Install IDS analysis tools
	The IDS will be able to detect and respond to unauthorized attempts to penetrate or deny use.	Set IDS to auto block
EN-11	The information system must provide the ability to specify and manage user access rights to the information system and data resources (i.e. access authorization through the network), supporting the organization’s security policy for access control.	Set group policy on networks
EN-16	The information system environment shall be capable of physically protecting the information system and components stored in a remote location by signaling the occurrence of fire, flood, power loss, and environmental control failures that might adversely affect information system operations.	Install automatic sensors with alert capability in data centers
PT-4	The IDS system should be sufficiently robust to detect replay attacks.	Install IDS with replay attack detection capability
SA-1	The information system security controls the number of concurrent sessions for any user to [define number of sessions].	Set concurrent sessions to [site-defined limitation]

Networked Systems		
Control	**Description**	**Action**
EN-9	The information system must have perimeter protection that implements a managed interface with any external connection, implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted.	Install a firewall at the network perimeter
	The information system denies information flow by default and allows information flow by exception (i.e., deny all, permit by exception).	Set firewall to deny by default
	The organization prevents the unauthorized release of information outside of the information system boundary, or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.	Set firewall to fail closed
PT-2	The organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.	Install encryption software
	The information system must incorporate a secure tunneling protocol capability between systems to protect information from unauthorized disclosure during transmission.	Configure secure tunnel between systems
TP-1	The information system must incorporate an NSA-approved secure tunneling protocol capability between systems to protect information from unauthorized disclosure during transmission.	Install an NSA-approved secure tunneling protocol or device between systems
	Two-factor authentication is required to establish a connection between remote systems.	Install two factor authentication on remote connections

PL 5-7		
Control	**Description**	**Action**
	A custom Trusted Computing Base (operating system) must be used that meets all requirements for PL 5-7 must be installed.	Install properly configured TCB on system(s)

Appendix 2

Continuous Monitoring Assessment Checklist

The following is a checklist of documentation, system processes, and technical controls that would be reviewed during a continuous monitoring assistance visit. The checklist activities are designed to be conducted in coordination with the sites ISSO and ISSM.

1. Review Master Plans, Certification and Accreditation package, MOUs/MOAs. Verify ATO has been received and is current.

2. Verify random sample of ISSO appointment letters.

3. Verify training – review database – interview personnel.

4. Verify that records and documentation requirements are being met.

5. Review process for the deployment of custom developed applications.

6. How many:
    a. Standalone desktops
        i. Are any of these networked in any fashion? If so, do they have their own SSP? If not, why?
    b. Laptops
    c. Faxes
    d. Periods processing systems
    e. Isolated networked systems
    f. Networked system

7. Choose random sample of SSPs from each of the system configuration types.
    a. Review the addendum for each system chosen.
        i. When was it accredited (w/in last 3 yr)?
        ii. Have any security significant changes occurred since it was accredited?
        iii. When was the last periodic security performance test plan completed?
        iv. Visit with the Line Mgmt for the system to see if they are aware of and understand the risks and associated mitigation for the system for which they are responsible.
        v. Do the Protection Levels and Levels of Concern for the systems match the way the system is being used?
        vi. Have any unique risks been identified and if so, what are the mitigating actions?
        vii. Does the DOE warning banner appear?
        viii. Review the maintenance logs.

1. Are they being used as noted in the security plan?

ix. Look at usage logs (if required by security plan).

1. Are they using manual or automatic monitoring (tracked by the security logs of the operating system)?
2. If manual, do usage logs match the check in/out sheet? If not, why?
3. If automatic, how do they document that the logs are reviewed? How often are the logs reviewed? What is tracked in the audit logs, and does it match what is required by the manual and SSP?

x. What is the backup process? Is it being followed?

xi. Is the configuration diagram current (if required by the security plan)?

xii. Are the hardware/software inventories correct?

b. Verify Code of Conduct and annual training/briefing has been completed within last 12 months for each user on the system.

i. Are these records kept w/the system book?

ii. What does the ISSO do for the annual briefing?

iii. Does each user on the system still have a need for access?

iv. How are user terminations handled?

c. Verify antivirus is loaded on each system.

i. Verify the virus definitions are updated at least annually.

ii. Does the ISSO have a different schedule for updates? If so, are they doing what they say (verify in the addendum vs. what ISSO says)?

d. Verify if there is any public domain software loaded on the system.

i. Does the ISSO have permission from the ISSM to use it?

ii. Look at approval for use.

e. Verify markings.

i. Front/back with level/category.

ii. Removable hard drives are marked on the carrier and inside on the actual hard drive.

iii. Do the workstations have the highest level/category affixed to the system and use the flip chart?

1. for laptops, do they have the Accredited Classified Laptop Computer Validation Card kept with the laptop?

iv. Are the In/Out cards being completed?

v. Are cases, sleeves, envelopes, etc marked top/bottom front/back with the highest level?

vi. Is unclassified material co-located w/classified? If so, is the unclassified material marked with the appropriate unclassified or UCI marking?

f. Verify separation distances.

i. Are cables appropriately marked?

ii. Are distances correct for red/black separations?

        iii. Is there sufficient space to conduct an inspection?

8. Identification and Authentication.
    a. M 471.2-2, VI.4j(3) states that user generated passwords are prohibited.
        i. What password generation tool is being used? Is it DAA approved?
        ii. If not using a tool, why not? Do you have a deviation in place allowing the use of user generated passwords?
        iii. How is password complexity enforced?
    b. M 471.2-2, VII.12a(2) discusses successive log attempts. How does security plan implement? Is it being followed?

9. Performance Testing.
    a. Check configuration using "gold disk" or other approved configuration management tool and document results.
    b. Create test account or have a user and administrator available on a sample of workstations (suggest different ISSOs)
        i. Log in with invalid ID.
        ii. Log in with invalid password.
        iii. Change password to all numbers, all alpha, all symbol.
        iv. Change password to less than 8 characters.
        v. What is lockout period? Is it documented in the addendum?
    c. Attempt exploits and results documented.
    d. Validate that notification of user changes to the system is completed.
    e. Perform IDS/IPS performance test.
    f. Perform vulnerability scans and document results.
    g. Perform social engineering test and document results.

10. Clearing, Sanitization, and Destruction
    a. Performance Test – periods process;
        i. User/ISSO question – What is the method for sanitization between periods? ANWSER: double power down.
        ii. Does the system have separate media for each level/category of data processed?
    b. Printers:
        i. Does the SSP cover printers with volatile memory which is consistent with M 205.1-2, Table 2. Does it also cover items such as printer ribbons, toner cartridges, and laser drums etc?
    c. Faxes:
        i. SSP says no sanitization is required if the fax machine does not have memory or image retention. Are toner cartridges sanitized? (M 205.1-2, CRD, Table 3 requires some kind of sanitization).
    d. ESM sanitization and destruction:
        i. Verify clearing/sanitation documentation (label) affixed includes (M 205.1-2, 3b):
            1. equipment description.

        2. review statement the equipment has been cleared and/or sanitized, and
        3. date, name, and signature of certifier.
    ii. Does the certifier have documented (M 205.1-2, 5a-d):
        1. media serial number, make, and model.
        2. classification level (if applicable).
        3. purpose for clearing and/or sanitation.
        4. procedures used.
    iii. Is degaussing accomplished with an NSA-approved Type 1 or 2 deguasser? Has the degausser been re-certified to assure it is purging data?
        1. What is maintenance process? Is it followed? Documented?
        2. What is the approval process for purged media?

11. Classified cyber security incidents.
    a. How many were reported in the last 24 months (period since last self-assessment)?
    b. Have any required reporting through the M 205.1-1 (IPWAR)? If so, how many?
    c. Have had occasion in which the system had to be shut down until incident completed? If so, review the incident(s) and the ISSM's approval to start processing again?

12. Faxes.
    a. Cover pages has level/category @ top/bottom, date of transmission, number of pages sent, sender/receiver name, company name/address, if not part of document, assure that "When separated from enclosure, handle this document as unclassified" is printed near bottom of cover page.
    b. Fax Logs for sent and received documents.

Appendix 3

Documentation Requirements

The following outlines the documents required for compliance with the SC NSS Program. The SC NSS Program is documented within the site Classified Cyber Security Program Plan ("Site SP") and associated procedures, which include:

- Site review
- Protection requirements
- Configuration management
- Awareness and training requirements
- Information marking requirements
- Storage requirements
- Visitor Access requirements
- Interconnected systems
- Program coordination
- Incident handling and response requirements
- Clearing, purging, and destruction requirements
- System Security Plans
- Certification and Accreditation (C&A) requirements
- Metrics

The following specific documentation is required within the NSS control sets:

Control	Documentation Required
All Systems	
AU-6	Audit record review and results. Audit records shall be reviewed at least weekly and retained for at least one year.
CM-1	Configuration management policy and process documentation. The CM documentation shall include a configuration list that describes the configuration items that comprise the information system and the method used to uniquely identify the configuration items.
CM-2	Configuration management tracking, including the information system implementation representation, design documentation, functional and security test documentation, user documentation, administrator documentation, and CM documentation (e.g., version and change log). The CM documentation shall describe how the configuration items are tracked by the CM system.
CM-8(2)	The organization develops, documents, and maintains a current inventory of the components of the information system and relevant ownership information.
DO-1	The system owner shall document procedures for delivery of the information system or parts of it to the user and shall use the delivery procedures. The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the information system or updates to the user's site.
DP-1	Any named object that is not controlled by the DAC security policy must be justified in the SSP.
DP-2	The PCSP or SSP must list the attributes that are used by the DAC policy for access decisions.

Control	Documentation Required
All Systems	
DV-1	The system owner shall provide a functional specification for systems other than Commercial Off-the-Shelf (COTS) software. The functional specification shall provide the high-level design. The system owner shall provide the high-level design (HLD) of the information system security controls. The HLD shall be internally consistent; shall describe the structure of the information system security controls in terms of subsystems; shall describe the security functionality provided by each subsystem of the information system security controls; shall identify any underlying hardware, firmware, and / or software required by the information system security controls with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software; shall identify all interfaces to the subsystems of the information system security controls; and shall identify which of the interfaces to the subsystems of the information system security controls are externally visible.
SA-5(1)	The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system. The organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.
SA-10	The organization requires that information system developers create and implement a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation.
EN-2	Access authorization, need-to-know, means for off line contact, mailing address, shall be validated annually.
EN-7	Procedures shall be established and documented to ensure the identification, collection, and preservation of data (at the system and network level) needed to analyze and reconstruct events resulting from penetration attempts, penetrations, and on-going cyber attacks and/or failures.
EN-13	Prior to their first access to information, each user's need-to-know shall be formally authorized by management, the data owner, or the data-steward.

Control	Documentation Required
All Systems	
EN-23	All authenticated users shall be trained to understand applicable information system use policies, the approved use of the information system, the vulnerabilities inherent in the operation of the information system, and their cyber security responsibilities.
GD-1	The system owner shall provide administrator guidance to system administrative personnel. The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the information system; shall describe how to administer the information system in a secure manner; shall contain warnings about functions and privileges that should be controlled in a secure processing environment; shall describe all assumptions regarding user behavior that are relevant to secure operation of the information system; shall describe all security parameters under the control of the administrator, indicating secure values as appropriate; shall describe each type of security relevant event relative to the administrative function that needs to be performed, including changing the security characteristics of entities under the control of the information system security controls; shall describe and be consistent with all other documentation supplied for evaluation; and shall describe all security requirements for the IT environment that are relevant to the administrator.
GD-2	The system owner shall provide user guidance. The user guidance shall describe the functions and interfaces available to the non-administrative users of the information system; shall describe the use of user-accessible security functions provided by the information system; shall contain warnings about user accessible functions and privileges that should be controlled in a secure processing environment; shall clearly present all user responsibilities necessary for the secure operation of the information system, including those related to assumptions regarding user behavior found in the statement of the information system security environment; shall be consistent with all other documentation supplied for evaluation; and shall describe all security requirements for the IT environment that are relevant to the user.
LC-1	The system owner shall produce development security documentation. The development security documentation shall describe all physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the information system design and implementation in its development environment, and shall provide evidence that these security measures are followed during the development and maintenance of the information system.

Control	Documentation Required
All Systems	
LC-2	The system owner shall document the flaw remediation procedures. The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the information system, and shall describe the methods used to provide flaw information, corrections, and guidance on corrective actions to information system users. The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided as well as the status of finding a correction to the flaw, and shall require that corrective actions be identified for each of the security flaws.
LC-2(1)	The system owner shall designate one or more specific points of contact for user reports and inquiries about security issues involving the information system. The flaw remediation procedures shall include a procedure requiring timely responses for the automatic distribution of security flaw reports and the associated corrections to registered users who might be affected by the security flaw. The flaw remediation guidance shall describe a means by which information system users may register with the system owner, to be eligible to receive security flaw reports and corrections. The flaw remediation guidance shall identify the specific points of contact for all reports and inquiries about security issues involving the information system.
LC-2a	The flaw remediation procedures documentation shall describe a means by which the system owner receives information system users' reports and inquiries of suspected security flaws in the information system. The procedures for processing reported security flaws shall ensure that any reported flaws are corrected, and the correction issued to information system users and shall provide safeguards that any corrections to these security flaws do not introduce any new flaws. The flaw remediation guidance shall describe a means by which information system users report to the system owner any suspected security flaws in the information system and a means for verification that suspected security flaws are addressed.
LC-3	The system owner shall establish a life-cycle model to be used in the development and maintenance of the information system and shall provide life-cycle definition documentation. The life-cycle definition documentation shall describe the model used to develop and maintain the information system and the life-cycle model shall provide for the necessary control over the development and maintenance of the information system.

Control	Documentation Required
All Systems	
MT-2	The PCSP or SSP must state the components of the access rights that may be modified, must state any restrictions that may exist for a type of authorized user, and the components of the access rights that the user is allowed to modify.
PT-3	The organization employs manual or automated mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure.
PT-8	The SSP shall specify those situations in which an audit is desired and feasible from the "secure" state.
TE-1	The system owner shall provide evidence of the test coverage. The evidence of test coverage shall show the correspondence between the test identified in the test documentation and the information system security controls as described in the functional specification.
TE-1(1)	The system owner shall provide an analysis of test coverage. The analysis of test coverage shall demonstrate the correspondence between the test identified in the test documentation and the information system security controls as described in the functional specification and between the information system security controls as described in the functional specification and the tests identified in the test documentation are complete.
TE-2	The system owner shall test the information system security controls and document the results. The system owner shall provide test documentation that consists of test plans, test procedure descriptions, expected test results, and the actual test results. The test plans shall identify the security controls to be tested and describe the goal of the tests to be performed. The test procedures shall identify the test to be performed, and describe the scenarios for testing each security function. The scenarios shall include any ordering dependencies on the results of other tests. The expected test results shall show the anticipated outputs from a successful execution of the tests. The test results from the system owner execution of the tests shall demonstrate that each tested security control behaved as specified. The system owner shall provide a suitable information system for testing, and shall provide an equivalent set of resources to those that were used in the system owner’s functional testing of the information system security controls.
TE-2(1)	The system owner shall provide the analysis of the depth of testing. The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the information system security controls operates in accordance with its high-level design.

Control	**Documentation Required**
	All Systems
VA-1	The system owner shall perform and document an analysis of the information system deliverables, searching for obvious ways in which a user can violate the information system security policy. The system owner shall document the disposition of the obvious vulnerabilities, and the documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the information system.
VA-1(1)	The system owner shall document the disposition of identified vulnerabilities. The documentation shall justify that the information system, with the identified vulnerabilities, is resistant to obvious penetration attacks.
VA-2	The system owner shall provide guidance documentation. The guidance documentation shall identify all possible modes of operation of the information system (including operation following failure or operational error), their consequences, and implications for maintaining secure operations. The guidance documentation shall be complete, clear, consistent, and reasonable; shall list all assumptions about the intended environment; and list all requirements for external security measures (including external procedural, physical and personnel controls).
VA-2(1)	The system owner shall document an analysis of the guidance documentation that demonstrates the guidance documentation is complete.
MP-6(1)	The organization sanitizes information system media, both digital and non-digital, prior to disposal or release for reuse. The organization tracks, documents, and verifies media sanitization and disposal actions.
MP-6(2)	The organization sanitizes information system media, both digital and non-digital, prior to disposal or release for reuse. The organization periodically tests sanitization equipment and procedures to verify correct performance.
CS-1	When cryptography is required and used within the information system for other than telecommunications, the information system security controls shall establish and manage cryptographic keys using automated mechanisms with supporting procedures or manual procedures. The requirements in DOE Manual 205.1-3, "*Telecommunications Security Manual*", must be implemented for telecommunications systems. If cryptographic keys are not used, this should be stated in the SSP.

Control	Documentation Required
PL 5-7	
CM-1(1)	The CM documentation shall include an acceptance plan that describes the procedures used to accept modified or newly created configuration items. The CM system shall support the generation of the information system, provide an automated means by which only authorized changes are made to the information system and CM implementation representation, and describe the automated tools used in the CM system.
CM-2(1)	The CM documentation shall show that the CM system tracks security flaws.
DO-2	The system owner (vendor) shall document procedures necessary for the secure installation, generation, and startup of the information system. The documentation shall describe the steps necessary for secure installation, generation, and start-up of the information system. The documentation shall confirm that the information provided meets all requirements for content.
DV-1(1)	The HLD shall describe the purpose and method of use of all interfaces to the subsystems of the information system security controls, providing details of effects, exceptions, and error messages as appropriate, and shall describe the separation of the information system into security control-enforcing components and other subsystems.
DV-2	The system owner shall provide the implementation representation for a selected subset of the information system security controls. The implementation representation shall unambiguously define the information system security controls to a level of detail such that the information system security controls can be generated without further design decisions. The implementation representation shall be internally consistent.
DV-3	The system owner shall provide an information system security policy model. The system owner shall demonstrate correspondence between the functional specification and the information system security policy model. The information system security policy model shall describe the rules and characteristics of all policies of the information system security policy that can be modeled, and include a rationale that demonstrates that it is consistent and complete with respect to all policies of the information system security policy that can be modeled. The demonstration of correspondence between the information system security policy model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the information system security policy model.

Control	Documentation Required
PL 5-7	
PE-8(2)	The organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) that includes: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; and (vii) name and organization of person visited. Designated officials within the organization review the visitor access records [Assignment: organization-defined frequency. The organization maintains a record of all physical access, both visitor and authorized individuals.]
SA-5(2)	The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system. The organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).

Control	Documentation Required
Supplemental for Integrity and Availability	
IR-2(1)	The organization trains personnel in their incident response roles and responsibilities with respect to the information system, and provides refresher training [Assignment: organization-defined frequency, at least annually]. The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.
IR-3(1)	The organization tests and/or exercises the incident response capability for the information system [Assignment: organization-defined frequency, at least annually] using [Assignment: organization-defined tests and/or exercises] to determine the incident response effectiveness and documents the results.
IR-5(1)	The organization tracks and documents information system security incidents on an ongoing basis.
PE-8(1)	The organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) that include: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; and (vii) name and organization of person visited. Designated officials within the organization review the visitor access records [Assignment: organization-defined frequency.]
SA-10	The organization requires that information system developers create and implement a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation.